

Claims

What is claimed is:

1. A method of migrating data encrypted using a first key set to data encrypted using a second key set, said method comprising:

decrypted data encrypted using a first key set; and

re-encrypting, by a data access control function within an integrated system, the data using a second key set.

2. The method of claim 1, wherein the data access control function comprises a hardware component of the integrated system.

3. The method of claim 1, wherein the decrypting is also performed by the data access control function of the integrated circuit.

4. The method of claim 1, further comprising retrieving for decryption, from storage associated with the integrated system, the data encrypted using the first key set.

5. The method of claim 1, further comprising modifying at least one operational characteristic associated with the data access control function, said at least one operational characteristic residing in an access table employed by the data access control function, and wherein the modifying includes modifying the access table to indicate that encrypted data in a current location is to be decrypted using the first key set, and is to be re-encrypted using the second key set when undergoing storage to a new data location.

6. The method of claim 1, wherein the decrypting and re-encrypting are responsive to the first key set having been used a predetermined count for at least one of encrypting and decrypting data, and wherein the method further comprises counting a number of times the first key set is employed in the at least one of encrypting and decrypting of data.

7. The method of claim 6, wherein the counting comprises employing a key usage counter maintained by the data access control function of the integrated system.

8. The method of claim 1, wherein the data encrypted using the first key set is received from a source external to the integrated system.

9. The method of claim 8, wherein the decrypting is performed in software within the integrated system, and wherein the re-encrypting, by the data access control function, is performed in hardware of the integrated system.

10. The method of claim 9, wherein the second key set is unique to the integrated system.

11. A system of migrating data encrypted using a first key set to data encrypted using a second key set, said system comprising:

means for decrypting data encrypted using a first key set; and

means for re-encrypting, by a data access control function within an integrated system, the data using a second key set.

12. The system of claim 11, wherein the data access control function comprises a hardware component of the integrated system.

13. The system of claim 11, wherein the means for decrypting is also performed by the data access control function of the integrated circuit.

14. The system of claim 11, further comprising means for retrieving for decryption, from storage associated with the integrated system, the data encrypted using the first key set.

15. The system of claim 11, further comprising means for modifying at least one operational characteristic associated with the data access control function, said at least one operational characteristic residing in an access table employed by the data access control function, and wherein the means for modifying includes means for modifying the access table to indicate that encrypted data in a current location is to be decrypted using the first key set, and is to be re-encrypted using the second key set when undergoing storage to a new data location.

16. The system of claim 11, wherein the means for decrypting and means for re-encrypting functions are responsive to the first key set having been used a predetermined count for at least one of encrypting and decrypting data, and wherein the system further comprises means for counting a number of times the first key set is employed in the at least one of encrypting and decrypting of data.

17. The system of claim 16, wherein the means for counting comprises means for employing a key usage counter maintained by the data access control function of the integrated system.

18. The system of claim 11, wherein the data encrypted using the first key set is received from a source external to the integrated system.

19. The system of claim 18, wherein the means for decrypting is performed in software within the integrated system, and wherein the re-encrypting, by the data access control function, is performed in hardware of the integrated system.

20. The system of claim 19, wherein the second key set is unique to the integrated system.

21. At least one program storage device readable by a machine embodying at least one program of instructions executable by the machine to perform a method of migrating data encrypted using a first key set to data encrypted using a second key set, said method comprising:

decrypting data encrypted using a first key set; and

re-encrypting, by a data access control function within an integrated system, the data using a second key set.

* * * * *